Dynamic Security-aware Routing for Zone-based data Protection in Multi-Processor System-on-Chips

Johanna Sepulveda*, Ramon Fernandes†, Daniel Florez‡, Cesar Marcon†, and Georg Sigl*§,
*Institute for Security in Information Technology, Technical University of Munich, Germany
†FACIN, Pontifical Catholic University of Rio Grande do Sul, Porto Alegre, Brazil
‡University of Los Andes, Bogota, Colombia
§Fraunhofer Institute for Applied and Integrated Security, Garching, Germany
johanna.sepulveda@tum.de

***Abstract*—In this work, we propose a NoC which enforces the encapsulation of sensitive traffic inside the asymmetrical security zones while using minimal and non-minimal paths. The NoC routes guarantee that the sensitive traffic is communicated only through the trusted nodes which belong to the security zone. As the shape of the zones may change during operation, the sensitive traffic must be routed through low-risk paths. We test our proposal and we show that our solution can be an efficient and scalable alternative for enforce the data protection inside the MPSoC.**

***Index Terms*—MPSoCs, Network-on-Chip, Security, Zones, Encapsulation.**

I. Introduction

Multi-Processors System-on-Chip (MPSoCs) are characterized by their flexibility and high computational capabilities. They integrate dozens of computation and storage Intellectual Property (IP) cores, which exchange information through a Network-on-Chip (NoC). Packets are exchanged from a source IP to a destination IP by means of a set of routers and links. MPSoCs are able to support several applications which may be stored on chip or downloaded through external networks as the Internet. The application is spread over the IPs of the MPSoC. Due performance and power constrains, such mapping may change during execution time. For critical applications, splitting the application into several IPs forces the sensitive data exchanging through the shared an unprotected NoC. This exposes data to attacks as shown in [1], [2].

MPSoCs are now target of several attacks. Malicious entities profit of the hyper-connectivity of Internet-of-Things (IoT) to download malware onto the MPSoC and infect IPs. Such kind of remote software-based attacks account for 70% of the security incidents in MPSoCs. Remote timing attacks belong to this category. Such attacks exploit the leakage caused by shared resources of the MPSoC: processing elements, memories and the communication structure. Sensitive communication at NoC must be protected. The work of [3] shows that by exploiting NoC communication collisions among sensitive and the attacker traffic, the secret key of the sensitive application may be retrieved.

Previous works have shown that NoCs can be enhanced with security mechanisms in order to prevent and mitigate attacks. Firewalls, customized network protocols and customized routers are used to built security zones. These zones encapsulate the sensitive traffic into trusted areas. They are constituted by a set of trusted IPs and routers, in which only sensitive and trusted traffic is exchanged. Thus, avoiding collisions with malicious traffic. Customizing the router by means of routing modification is one of the most effective techniques to built security zones and protect the traffic [2], [3]. In [2] the authors propose dynamic risk-based routing to encapsulate the traffic in low-risk paths. The risk value is provided by the number of firewall activations. Despite the fast runtime configuration, the lowest-risk path can not be guaranteed due the minimal path constraint. In [3] a design time approach based on region routing is used for guaranteeing the encapsulation of traffic inside asymmetric security zones. However, this approach is not suitable for reshaping the security zones at runtime.

In order to overcome such drawbacks, in this work we NOE-RNoC, an architecture that combines region-based routing (design time) and non-minimal adaptive routing (runtime) to efficiently encapsulate sensitive traffic.

The contributions of this work are:

- Implementation of a non-minimal adaptive routing technique guided by the security metric: risk of the hop.
- Fast reconfiguration of a region-based routing
- Evaluation of performance, cost and security.

This paper is divided into seven sections. Section II presents the previous works on NoC-based security. Section III describes the MPSoC and the threat model. Section IV presents the mechanisms for security zones protection. Section V presents the architecture of NOE-RNoC. Section VI shows the experimental work and results. Finally, Section VII presents the conclusions.

II. Related Works

Security integration at NoC-based architectures has been shown as an effective solution to protect heterogeneous MPSoCs. Such mechanisms avoid unauthorized data modification, extraction and system service deny. Security zones can be implemented though the NoC resources. The goal is to protect the MPSoC by encapsulating the sensitive traffic into trusted areas. The works of [3], [4] use routing to encapsulate the sensitive traffic. The authors of [3] present a region-based routing approach based on the security characteristics of the application. Despite the good results, it does not consider security zone reshaping during runtime. In the work of [4] the risk metric is used to guide the routing of sensitive traffic. The risk of the path is evaluated at the destination interface. When a risk threshold is exceeded a new low-risk path is explored. Four routing alternatives are used (deterministic, hop-based, weighted and bounded). All these routing algorithms are

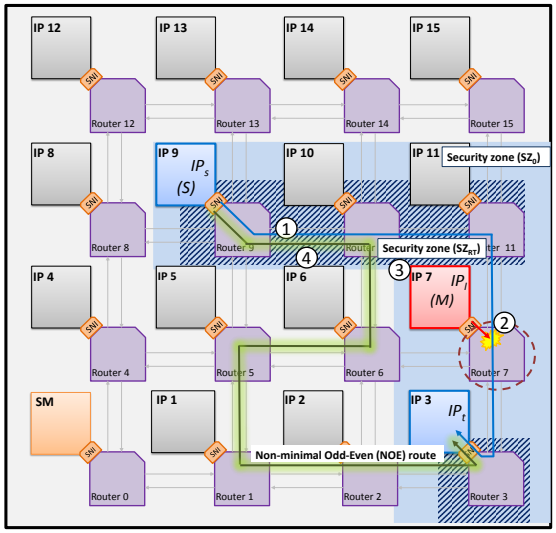

Fig. 1: Example of a 16-IP cores MPSoC.

constrained by the minimal path, thus restricting the search of low-risk paths.

III. MPSoC description and threat model

MPSoCs integrate a set of IP cores that process and store data in order to execute an application. Such application are divided into tasks and split on the IPs of the MPSoC. The communication among the IPs is performed through the NoC, a network of routers and links inside the chip. Fig. 1 shows an example of an MPSoC of 16-IP cores linked through a 16-router NoC. The communication between the IP target (IP_t) linked at router (R_3) and IP source (IP_s) linked at router (R_9) requires 5 commutations on the NoC $(R_9, R_{10}, R_{11}, R_7, R_3)$.

We consider that the MPSoC executes a sensitive (S) and other types of applications simultaneously in the same chip. S is split into the cores IP_9 and IP_3, thus forcing the communication of sensitive data through the NoC (1). The NoC path used to communicate the sensitive data is called sensitive path. The sensitive path of Fig. 1 is constituted by the routers $(R_9, R_{10}, R_{11}, R_7, R_3)$. The NoC and interfaces are considered secure. That is, the attacker cannot modify their behavior.

The attacker can infect the IP cores by executing a malicious application (M) into the MPSoC. Malicious task may be installed on an IP, thus turning it into an infected IP (IP_I). Fig. 1 shows the infected IP_7, which is linked directly to a router inside the sensitive path. The attacker is able to control the traffic injection and to monitor the IP_I throughput. As showed in [5], [6], an attacker may exploit communication collisions between the sensitive and malicious traffic to perform timing attacks. Collisions allow that the attacker recognizes the traffic pattern of the sensitive traffic by means of the degradation of the throughput of the (IP_I). The collision in Fig. 1 takes place at R_7 (2). As a result, the authors of [5] have shown that by observing the traffic due 76 AES encryption, IP_I is able to retrieve 12 of the 16 bytes of the secret key. Complementary brute force attack can be used to reveal the complete secret key.

In order to perform the attack, the following preconditions are required:

- Attacker is able to infect an IP of the MPSoC.
- Attacker can control the traffic generation and monitoring of the infected IP.
- Infected IP is in the sensitive path.

IV. Mechanisms for Security Zones protection

A security zone *SZ* is a physical space (continuous or disrupted) that wraps and isolates the IPs that execute sensitive applications. IPs that belong to the SZ are considered trusted among them. The task mapping of sensitive applications inside the MPSoC defines the shape of the SZ. However, if a trusted IP is attacked or the mapping of the application is modified at runtime, the SZ must be reshaped. In order to create the SZ, the NoC routing can be employed. The routing logic selects the router output for the granted input. Therefore, it can be used to restrict the communication through the hops inside the security zone. Reshaping the SZ implies into the NoC routing modification in runtime. The new route must be secure.

Firewalls embodied in the NoC interfaces are commonly used to protect the traffic and enforce the security policy of the system. This information can be use to detect possible points of attack and to drive the runtime modification of the NoC routing. Fig. 1 shows an initial continuous SZ_0 (1) that includes the $(IP_9, IP_{10}, IP_{11}, IP_7, IP_3)$. However, IP_7 is infected at runtime and detected by the firewalls (2), which trigger a reshape of the SZ. The infected IP is removed from the SZ and a new disrupted SZ is created (SZ_{RT}) as in (3). A new sensitive path is computed (4), which requires 7 commutations on the NoC $(R_9, R_{10}, R_6, R_5, R_1, R_2, R_3)$. In this work we propose the architecture able to establish and modify SZ as well as to reroute the sensitive traffic through non-minimal routes driven by the risk level of each hop.

In this paper we propose a NoC architecture able to support dynamic security zones and protected communications inside the MPSoC by combining a region-based routing (at design time) and Non-minimal Odd-Even routing (at runtime).

A. Region-based routing (design time)

The region-based routing forces that the communication paths of any pair of IP cores that belong to the same security zone is performed inside the zone. Determining the routes inside a region while guaranteeing deadlock-free routes is a complex task. The Segment-based Routing (SBR) and Region-based Routing (RBR) algorithms are used to determine the routes for encapsulating the traffic into a region. SBR is responsible for deadlock prevention and IP cores reachability, while RBR computes the routing tables. SBR is composed of two steps: (i) segment computation, that splits the NoC into segments characterized by a turn restriction to avoid deadlocks; and (ii) placement of routing restrictions. RBR uses the turn restrictions computed by SBR to find paths between all origins and destinations in the NoC. It includes three steps: i) routing computation, for each source-target IP cores pair; ii) region computation, that joins at each router multiple routing entries based on the input and output port values; and iii) region merge, which merges overlapping routing entries in order to reduce the size of the routing tables. Designer can

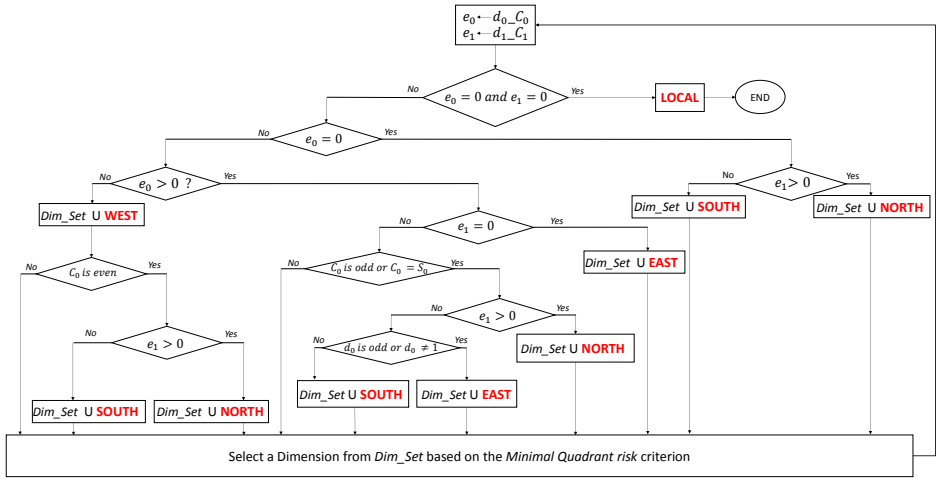

Fig. 2: Non-minimal adaptive odd-even turn model (NOE).

decide the IP core members of the SZ and the mapping on the MPSoC. The SBR is used to compute the segments and turn restrictions required to keep the traffic inside a security zone. The goal is to create the smallest possible segments that contain elements from the same security zone. The RBR searches the paths between each pair of IP_s and IP_t and creates the routing tables (RBR tables) for each hop. Such a network of hopes constitute the RNoC. More details about the algorithm can be found in [3].

The high complexity of SBR and RBR turns prohibitive the utilization of such algorithms in runtime. Thus, when the security changes, a lighter approach must be used to find a low-risk path for the sensitive traffic.

B. Non-minimal Odd-Even NOE routing (runtime time)

NOE is a low-cost adaptive routing algorithm, able to follow different paths between a given IP_s, IP_t pair. It is a deadlock-free adaptive approach that restricts the locations at which the turns can be performed. It is based on two rules [7]:

- $Rule1$: Any packet is not allowed to take an $E-N$ turn at any nodes located in an even column, and it is not allowed to take an $N-W$ turn at any nodes located in an odd column.
- $Rule2$: Any packet is not allowed to take an $E-S$ turn at any nodes located in an even column, and it is not allowed to take an $S-W$ turn at any nodes located in an odd column.

The behavior of NOE is shown in Fig. 2. NOE analyzes and compares the packet destination (d_0, d_1) and the current router position (c_0, c_1) in order to select the proper router output port. Packets can be routed adaptively in East, West, North or South directions. NOE can be used to find a low-risk path for sensitive packets at runtime. The routing decision can be driven by the risk value of the hops. At the NOE-RNoC, each hop quantifies the weighted risk value of the four quadrants as shown in [4]. The value of the neighbors' risk together with the turn restriction, are taken into account to select the next hop. This technique avoids that the packets are trapped into dangerous paths. Each time the risk value of a hop is updated, the new value is broadcasted into the NoC hops that belong to the column and row. The implementation of adaptive routing may present higher costs when compared to deterministic approaches. However, adaptation may become mandatory for reliability purposes and so the cost overhead acceptable.

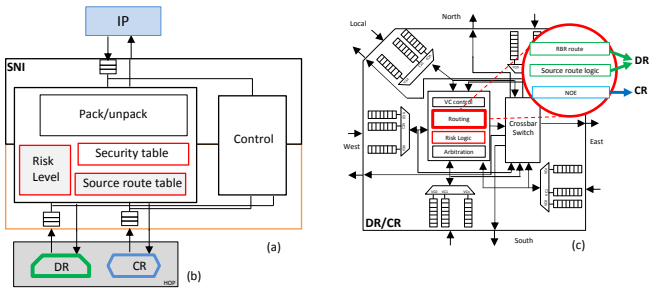

Fig. 3: Microarchitecture of SNI and Hops.

V. NoC Architecture

In this paper we propose NOE-RNoC, a security enhanced NoC to protect sensitive traffic inside the MPSoC. Sensitive traffic is encapsulated dynamically through low-risk paths inside a security zone. At design time, the region-based routing NoC (RNoC) is used to determine the routing table. At runtime, new sensitive paths are created through NOE routing driven by the risk metric. The protected NOE-RNoC is based on a two-level NoC composed of three main components: Secure network interfaces (SNI), Hops and Security Manager (SM). Their microarchitecture is shown in Fig. 3.

Secure network interfaces (SNIs): They implement the communication protocol (pack/unpack, route table, control) and security checking by means of firewalls (security table). The packet structure is composed of 6 fields: i) source, to identify IP_s; ii) destination, to identify IP_t; iii) route, to store the secure route; iv) risk threshold, contains the maximum risk allowed per hop; v) operation, to identify the type of packet (control, data write, data read); and vi) payload, that

is the data to be exchanged. The communication security is enforced by the firewall-based traffic inspection. Each time a packet is injected or received, the security checking is performed. At the source IP, the access control is performed by verifying the destination and operation fields of the packet. At the destination IP, the authentication is performed by checking the source and operation fields. When the security rules are violated, the firewall generates a notification which will increase the risk value of the hop: i) at source hop, when the attack is identified at the source network interface; or ii) at the hops used by the malicious packet, when the attack is identified at the destination network interface. Each time a new application is mapped on the system, the risk level of the hops linked to the modified IPs is restarted.

Hops: Integrate the Data Routers (DR) and Control Routers (CR) to exchange data and control signals. It also includes the RISK logic block, used to quantify and store the risk value of each hop as in [4]. Fig. 3 shows the router structure. The difference between DRs and CRs is the link size and the routing implementation. DRs route the packets by means of the RBR tables, or by source routing (data inside the route field of the packet). CRs use the RBR tables and NOE (used only for seeker packets). Each hop stores two risk values: $localrisk$ (hop risk) and $quadrantrisk$ (risk of the line and column neighbors). Local risk is used to determine if a hop is dangerous. Each time a sensitive packet uses a DR, the local risk is compared to the risk threshold value. If exceeded, the packet is sent back to the IP_s and the Security Manager is notified. The quadrant risk is used for the NOE routing. Quadrants that force the transition between security zones are penalized in order to favor the routing inside a single security zone.

Security manager (SM): It is a light software layer executed in a trusted IP in charge of configuration of the firewalls and control of the recovery mechanism under a possible attack. It includes the untrusted hop removal from a security zone.

During execution, the risk of a hop can be measured as in [4]. The risk is defined as the probability that a malicious process spies, denials the communication or corrupts the data in a NoC hop. The risk is measured by the amount of firewall notifications due the violation of security rules. When the risk of a hop inside the SZ overcomes the $RISKlevel$ value, defined by the designer, the hop is removed from the SZ. Therefore, the IP cores of the SZ that use the removed hop must search for an alternative low-risk path. These IPs inject a seeker packet which is commuted through the CR. The routing decision at each hope is based on the NOE algorithm that includes the risk value of each hop of the NoC. The route is stored by the seeker packet and then stored into the source route table of the SNI. The remove of the hops and the control of the seek process is performed by the security manager (SM).

VI. Experiments and Results

NOE-RNoC is modelled in SystemC-TLM and VHDL-RTL by extending the NoC design framework presented in [4]. SHOC is a modular cycle accurate simulation environment which supports a wide variety of components required for MPSoC simulation. This environment includes libraries of MPSoC attacks and tools for power and area estimation. NOE has been evaluated under three conditions: scalability, performance and security. NOE-RNoC is compared with the approaches proposed in [4].

Fig. 4 shows the impact of setting a new route by using the NOE and the previous approaches for different NoC sizes. The path length is equivalent to the diameter of the NoC. Results are expressed as a percentage of the exhaustive route search. Lower latency values represent efficient routing techniques. Results show that NOE is scalable. Only hop-based and deterministic approaches overcome NOE. These approaches do not require the risk status broadcasting. Oblivious neighbor risk approaches may limit the search of low-risk paths. Among the approaches where hops are aware of the NoC risk (weighted and bounded), NOE presents the best performance. NOE enhances the performance up to 8% and 15%, respectively, when compared to the weighted and bounded approaches.

The performance evaluation was carried out on an MPSoC that supports 5 applications (MG, IS, LU, FT, CG) of the NASA Numerical Aerodynamic Simulation (NAS) Benchmark. Fig. 5 shows the MPSoC mapping obtained by Cafes [8]. This tool optimizes the MPSoC mapping according to performance and power metrics. Each application is grouped into a single and continuous security zone. During operation time, 2 IP cores from each security region start to behave malicious. This experiment emulates the presence of hardware Trojans on the MPSoC. Thus, the routing inside the security regions must be modified.

Fig. 6 shows the performance result of the NOE-RNoC under uniform traffic with different injection rates. The path reconfiguration was forced during 25% of the operation time. The results show that NOE achieves the best performance results, overcoming the hop-based approach. Despite NOE-RNoC requires the broadcast of the risk values of the hops in order to quantify the quadrant risk, the performance of the applications is not affected. NOE employs the CR for all the extra communication. Moreover, the path found by the hop-based approach falls into infected hops that were performing timing attack (heavy traffic injection to detect the degradation of throughput), thus degrading the performance of the sensitive path. NOE, was able to avoid such hops.

The area, power and performance overhead of the security mechanisms are summarized in Table I as a percentage of the penalty of each configuration when compared to the MPSoC without protection. Results show that NOE presents the best trade-off among the alternatives that are NoC risk-aware.

For the security evaluation, our approach was evaluated under four kinds of attacks. Table II shows the results of the security evaluation. Higher values of attack avoidance represent a better level of protection. Results show that NOE and Bounded approaches achieve the highest protection levels for all the attacks.

VII. Conclusion

In this work we propose NOE-RNoC, a security enhanced NoC architecture that combines region routing and non-minimal risk-based routing technique to encapsulate sensitive traffic through low-risk paths. We present three main contributions. Firstly, we implement a non-minimal routing

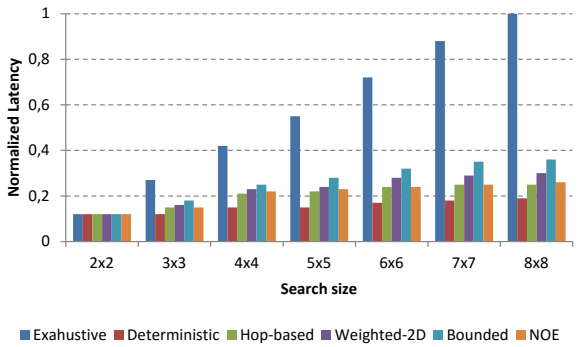

Fig. 4: Results of the scalability of the approaches.

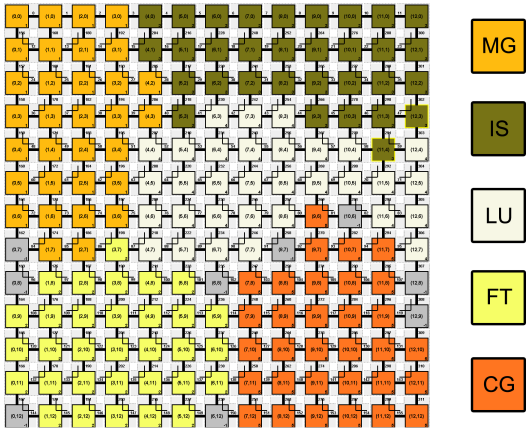

Fig. 5: Mapping of NAS benchmark in the MPSoC.

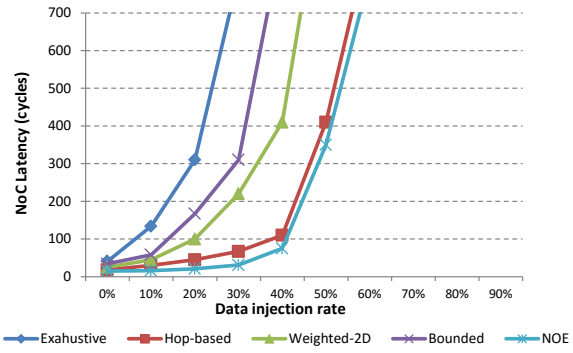

Fig. 6: performance results.

technique driven by low-risk metric. Secondly, we show that our architecture is able to protect the sensitive traffic even when some IP cores inside the security zones are tampered. Thus NOE-RNoC is able to find at runtime. Thirdly, we show that our NOE-RNoC is efficient and able to protect the sensitive traffic. Future work aims to explore other non-adaptive weighted routing techniques for finding secure paths efficiently.

TABLE I: Overhead when compared to a simple two-level NoC

Configuration	*Latency*	*Area*	*Power*
Deterministic	6,5%	9,6%	12,3%
Hop-based	8,3%	6,4%	5,1%
Weighted-2D	12,6%	14,3%	8,5%
Bounded	14,3%	8,6%	7,3%
NOE	7,8%	7,2%	5,8%

TABLE II: Security evaluation results

Attack scenario	*Exahus.*	*Hop*	*Weigh.*	*Bound.*	*NOE*
Overwrite memory	100%	100%	100%	100%	100%
Read mem.	100%	100%	100%	100%	100%
Repeated packet	100%	86%	84%	100%	100%
Wrong dest.	100%	87%	93%	100%	100%

References

[1] J. Sepulveda, D. Florez, and G. Gogniat, "Efficient and flexible noc-based group communication for secure mpsocs," in *2015 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Dec 2015, pp. 1–6.

[2] J. Sepúlveda, D. Flórez, and G. Gogniat, "Reconfigurable security architecture for disrupted protection zones in noc-based mpsocs," in *Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), 2015 10th International Symposium on*. IEEE, 2015, pp. 1–8.

[3] R. Fernandes, R. Cataldo, C. Marcon, G. Sigl, and J. Sepúlveda, "A security aware routing approach for noc-based mpsoc," in *Integrated Circuits and Systems Design (SBCCI), 2016 29th Symposium on*. IEEE, 2016, pp. 1–6.

[4] J. Sepúlveda, D. Flórez, R. Fernandes, C. Marcon, and G. Sigl, "Towards risk aware nocs for data protection in mpsocs," in *Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), 2016 11th International Symposium on*. IEEE, 2016, pp. 1–8.

[5] C. Reinbrecht, A. Susin, L. Bossuet, and J. Sepulveda, "Gossip noc - avoiding timing side-channel attacks through traffic management," in *IEEE Computer Society Annual Symposium on VLSI (ISVLSI '16)*, July 2016.

[6] M. Sepulveda, J.-P. Diguet, M. Strum, and G. Gogniat, "Noc-based protection for soc time-driven attacks," *Embedded Systems Letters, IEEE*, vol. 7, no. 1, pp. 7–10, March 2015.

[7] G.-M. Chiu, "The odd-even turn model for adaptive routing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 7, pp. 729–738, Jul. 2000. [Online]. Available: http://dx.doi.org/10.1109/71.877831

[8] C. Marcon, N. Calazans, E. Moreno, F. Moraes, F. Hessel, and A. Susin, "Cafes: A framework for intrachip application modeling and communication architecture design," *Journal of Parallel and Distributed Computing*, vol. 71, no. 5, pp. 714 – 728, 2011, networks-on-Chip. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731510002005